Risk Management Policy

VCAP-ISP-08

DOCUMENT AND RECORD CONTROL

Version Control

Document Control ID	VCAP.ISP-08_Risk Management Policy
Issued Date	29-September-22
Effective Date:	29-September-22
Owner:	ISMS DEPARTMENT

Revision Table

Date	Version	Brief Description	Author
07-September-21	0.1	Risk Management Policy – Draft	Lakshmi Balaji
29-September-21	1.0	Risk Management Policy	Lakshmi Balaji

Release Authorization

Task	Author	Title
Prepared by	Lakshmi Balaji	Deputy Vice President

Reviewer Authorization

Name	Title	Signature	Date
Mr. Prasenjit Datta	Head of Technology	Prasenjit Datta	29-September-2022

Approval Authorization

Name	Signature	Date
Mr. Prasenjit Datta	Prasenjit Datta	29-September-2022

Important Note: This document is intended solely for the use of the individual or entity to whom it is transmitted to, and others authorized to receive it. It may contain confidential or legally privileged information. If you are not the intended recipient you are hereby notified that any disclosure, copying, distribution or taking any action in reliance on the contents of this document is strictly prohibited and may be unlawful. If you have received this document in error, please notify us immediately.

TABLE OF CONTENTS

1. Office of Responsibility

Vice President, Information Security & Risk.

2. Purpose

As stated in the Company Information Security Program Charter, the Company will follow a risk management approach to developing and implementing Information Security policies, standards, guidelines, and procedures. The Information Security Program is designed to protect information assets by developing Information Security policies to identify, classify, and define the acceptable use of company information assets.

This Risk Management Policy defines the Company's endeavours to secure company information systems that store, process, or transmit Company or client information. Assist Company management with making well-informed risk management decisions, justify expenditures related to information system resources; assist Company management in authorizing (or accrediting) information systems on the basis of supporting risk management documentation.

3. Scope

The Policy applies to all employees, contractors, consultants, and vendors who access, use or control company resources.

4. Policy

4.1 Objectives

- The Company's risk management program encompasses three core processes: Risk Management, Risk Assessment, and Risk Mitigation.

- Risk management efforts support company management by balancing the operational and economic costs of protecting Company information systems and data while supporting the Company's mission. Specific instructions and requirements for conducting core risk management efforts are provided in the Risk Management Standard.

- Risk assessment efforts shall be utilized to determine the extent of potential threats and risks associated with company environments and information systems. The Company shall also assess the potential risk of engaging with third-party vendors. Specific instructions and requirements for conducting risk assessment efforts are provided in the Risk Management Procedure and the Third-Party Supplier Policy.

- Risk mitigation involves prioritizing, evaluating, and implementing appropriate risk-reducing controls as discovered from the risk assessment process. Specific instructions and requirements for risk mitigation efforts are provided in the Risk Mitigation Standard.

- Effective risk management efforts shall be integrated into the System Development Life Cycle. Refer to the System Development Life Cycle Standard for further information.

- For risk management efforts designed to address Company operations and facilities, refer to the Facility Review & Risk Assessment Process Standard.

- For risk management efforts designed to support operational remittance compliance and other related requirements, refer to the Anti-Fraud Standard, Anti-Money Laundering Standard, and Foreign Anti-Corruption Standard.

5. Related Policies

- Information Security Program Charter
- Security Awareness Training Standard

6. Policy Compliance

6.1 Responsibilities

- Chief Executive Officer (CEO) & Board members are the approval authority for the Risk Management Policy.
- The Vice President of Information Security & Risk is responsible for the development, implementation, and maintenance of the Risk Management Policy.
- Company management is accountable for ensuring that the Risk Management Policy and associated standards and guidelines are properly communicated and understood within their respective organizational units. Company management is also responsible for defining, approving, and implementing procedures in its organizational units and ensuring their consistency with the Risk Management Policy and associated standards and guidelines.
- All individuals, groups, or organizations identified in the scope of this policy are responsible for familiarizing themselves with the Risk Management Policy and complying with its associated policies.

7. Policy Enforcement and Compliance

Compliance with this policy is mandatory and Vivriti department managers shall ensure continuous compliance monitoring within their department. Compliance with the statements of this policy is a matter of periodic review.

Any breach of this policy may constitute a security violation and gives Vivriti the right to conduct disciplinary and / or legal action, up to and including termination of employment or business relationship.

Disciplinary action will be dependent upon the severity of the violation which will be determined by the investigations.

8. Waiver Criteria

This policy is intended to address information security requirements. If needed, waivers shall be formally submitted to the Information Security Management, including justification and benefits attributed to the waiver by the CEO.

The policy waiver shall be granted for a period of four months initially and shall be reassessed thereafter and can be extended up to a period of three consecutive terms. No waiver shall be provided for more than three consecutive terms on any of the policies.

9. Document Management

Technological advances and changes in the business requirements will necessitate periodic revisions to documents. Therefore, this document may be updated to reflect changes or define new or improved requirements as and when required and in compliance with the Information Security Program Charter.

Any change will require the approval of the Information Security Steering Committee (ISSC).

10. Glossary

Term	Definition
Information Security	The preservation of confidentiality, integrity and availability of information; in addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.
Policy	A plan of action to guide decisions and actions. The term may apply to government, private sector organizations and groups, and individuals. The policy process includes the identification of different alternatives, such as programs or spending priorities, and choosing among them on the basis of the impact they will have.

---End of Document---